ABSTRACT

A method of decrypting a message encrypted using a truncated ring cryptosystem. The method comprises selecting a window parameter T determining a plurality of windows of a predetermined size, each window being shifted by an amount less than or equal to the window parameter T. A decryption candidate is determined for each possible window. Each decryption candidate is tested to determine whether it is a valid message. The result of the decryption is chosen to be a valid message found in the previous step or if no valid message is found it is indicated that the message could not be decrypted. By this method, a constant number of decryption candidates are determined for each decryption.